CLAIMS

1. A method for providing authentication when messages are sent between an electronic communication apparatus (1) and a server (3, 41, 51, 61) according to a synchronization protocol, **characterized in that** an authentication method indicator (AMI) is incorporated in an authentication protocol of the synchronization protocol, wherein said AMI specifies an authentication method according to which the authentication is executed.

2.The method according to claim 1, wherein the AMI is incorporated in the meta command of the synchronization protocol and based on the authentication capabilities of the apparatus (1).

3. The method according to claim 1 or 2, wherein at least one authentication capability of the electronic communication apparatus is indicated in an authentication method list of an initialization message sent to the server (31, 41, 51, 61) for establishing a connection.

4. The method according to any of the previous claims, wherein any authentication data relating to the specified authentication method is incorporated in a data string of the synchronization protocol.

5. The method according to any of the previous claims, wherein the specified authentication method is GSM SIM authentication.

6. The method according to any of the claims 1-4, wherein the specified authentication method is UMTS USIM authentication, which also provides server authentication.

7. The method according to any of the claims 1-4, wherein the specified authentication method is WPKI or WIM authentication.

8. The method according to any of the claims 1-4, wherein the specified authentication method is SecureId or SafeWord authentication.

9. The method according to any of the claims 3-7, wherein the server (31, 41, 51, 61) determines the authentication capabilities of the electronic communication apparatus (1) based on the at least one authentication method listed in the authentication method list.

10. The method according to claim 9, wherein the server (31, 41, 51, 61) executes any necessary authentication steps according to one of the at least one authentication methods indicated in the authentication method list, and prepares and transmits a message to the electronic communication apparatus (1), comprising the AMI and any authentication data relating to the specified authentication method, in the data string of the message.

11. The method according to claim 10, wherein the electronic communication apparatus (1) receives the message, executes any necessary authentication steps according to the authentication method indicated by the AMI to generate an expected result, and prepares and transmits a response to the server, comprising the AMI, and any authentication data in the data string of the message.

12. The method according to any of the claims 1-6 and 9-11, wherein integrity protection is provided by utilizing CKs/IKs (cipher keys/integrity keys) generated by the electronic communication apparatus (1) and the server (31,

REPLACED BY
ART 34 AMDT

41, 51, 61), respectively, when SIM/USIM authentication is executed, which CK/IK is used for generating MAC values and using a hashing function for computing a HMAC on the entire message to be sent.

13. The method according to any of the claims 7 or 9-11, wherein integrity protection is provided in that the server generates a good integrity key, which is encrypted with the public key of the electronic communication apparatus (1), which is generated during the authentication procedure, said integrity key is sent to said apparatus (1), and utilized for generating MAC values and using a hashing function for computing a HMAC on the entire message to be sent.

14. The method according to claim 12 or 13, wherein the MAC value is computed as per RFC2104.

15. The method according to any of the claims 12-14, wherein the method utilizes SHA-1 as the hashing function.

16. The method according to any of the previous claims, wherein the protocol is the SyncML-DM protocol or the SyncML-DS protocol.

17. The method according to any of the previous claims, wherein the protocol is the Obex, http, or WSP protocol.

18. An electronic communication apparatus adapted to provide authentication when messages are exchanged with a server according to a synchronization protocol, **characterized in that** the apparatus is further adapted to incorporate an authentication method indicator (AMI) in the authentication protocol of the synchronization protocol for

indicating a specific type of authentication method, according to which the authentication is executed.

19. The apparatus according to claim 18, wherein the apparatus (1) is further adapted to send an initialization message to the server for establishing a connection, which message indicates the authentication capabilities of the apparatus.

20. The apparatus according to claim 19, wherein the initialization message comprises an authentication method list having at least one authentication method listed, type of apparatus, and/or identity of the apparatus (1).

21. The apparatus according to claim 18, wherein the apparatus (1) is further adapted to determine the type of authentication method to use from the authentication method indicator of a message received from the server (31, 41, 51, 61).

22. The apparatus according to any of the claims 18-21, wherein the apparatus (1) is further adapted to execute any of the steps necessary according to the specified authentication method.

23. The apparatus according to claim 22, wherein the apparatus (1) is further adapted to incorporate any authentication data in a data string of the message to be sent according to the synchronization protocol.

24. The apparatus according to any of the claims 18-23, wherein the apparatus (1) is further adapted to provide integrity protection by utilizing an IK (integrity key) for generating a MAC, and utilizing a hashing function for computing a HMAC on the entire message.

REPLACED BY ART 34 AMDT

25. The apparatus according to claim 24, wherein the apparatus (1) is adapted to compute the MAC value as per RFC2104.

26. The apparatus according to claim 24 or 25, wherein the apparatus (1) is further adapted to utilize SHA-1 as the hashing function.

27. The apparatus according to any of the claims 18-26, wherein the protocol is the SyncML-DM protocol or the SyncML-DS protocol.

28. The apparatus according to any of the claims 18-26, wherein the protocol is the Obex, http, or WSP protocol.

29. The apparatus according to any of the claims 18-28, wherein the apparatus (1) is further adapted to utilize GSM SIM authentication as the authentication method.

30. The apparatus according to any of the claims 18-28, wherein the apparatus (1) is adapted to utilize UMTS USIM authentication as the authentication method and provide server authentication.

31. The method according to any of the claims 18-28, wherein apparatus (1) is further adapted to utilize SecureId, SafeWord, WPKI or WIM authentication as the authentication method.

32. The apparatus according to any of the claims 18-31, wherein the apparatus is a pager, an electronic organizer, or a smartphone.

33. The apparatus according to any of the claims 18-31, wherein the apparatus is a mobile telephone (1).

34. A server adapted to provide authentication when messages are exchanged with an apparatus (1) according to a synchronization protocol, **characterized in that** the server (31, 41, 51, 61) is further adapted to incorporate an authentication method indicator (AMI) in the authentication protocol of the synchronization protocol for indicating an authentication method, according to which the authentication is executed.

35. The server according to claim 34, wherein the server (31, 41, 51, 61) is further adapted to incorporate any authentication data in a data string of the synchronization protocol.

36. The server according to claim 34 or 35, wherein the server (31, 41, 51, 61) is further adapted to determine from a received initialization message the authentication capabilities of the apparatus (1) and further determine a specific authentication method to utilize therefrom.

37. The server according to claim 36, wherein the server (31, 41, 51, 61) is further adapted to execute authentication according to the determined authentication method.

38. The server according to any of the claims 34-37, wherein the server (31, 41, 51, 61) is further adapted to provide integrity protection by utilizing an IK (integrity key) for generating a MAC, and utilizing a hashing function for computing a HMAC.

39. The server according to claim 38, wherein the server (31, 41, 51, 61) is adapted to derive the MAC value as per RFC2104.

40. The server according to claim 38 or 39, wherein the server (31, 41, 51, 61) is further adapted to utilize SHA-1 as the hashing function.

41. The server according to any of the claims 34-40, wherein the protocol is the SyncML-DM prctocol or the SyncML-DS protocol.

42. The server according to any of the claims 34-41, wherein the protocol is the Obex, http, or WSP protocol.

43. The server according to any of the claims 34-42, wherein the server (31, 41, 51, 61) is further adapted to utilize GSM SIM authentication as the authentication method.

44. The server according to any of the claims 34-42, wherein the server (31, 41, 51, 61) is further adapted to utilize UMTS USIM authentication as the authentication method and provide server authentication variable to the electronic user equipment (1).

45. The server according to any of the claims 34-42, wherein server is further adapted to utilize SecureId, SafeWord, WPKI or WIM authentication as the authentication method.